

QUICKLY CONSTRUCTING CURVES OF GENUS 4 WITH MANY POINTS

EVERETT W. HOWE

ABSTRACT. The *defect* of a curve over a finite field is the difference between the number of rational points on the curve and the Weil–Serre bound for the curve. We present a construction for producing genus-4 double covers of genus-2 curves over finite fields such that the defect of the double cover is not much more than the defect of the genus-2 curve. We give an algorithm that uses this construction to produce genus-4 curves with small defect. Heuristically, for all sufficiently large primes and for almost all prime powers q , the algorithm is expected to produce a genus-4 curve over \mathbf{F}_q with defect at most 4 in time $\tilde{O}(q^{3/4})$.

As part of the analysis of the algorithm, we present a reinterpretation of results of Hayashida on the number of genus-2 curves whose Jacobians are isomorphic to the square of a given elliptic curve with complex multiplication by a maximal order. We show that a category of principal polarizations on the square of such an elliptic curve is equivalent to a category of right ideals in a certain quaternion order.

1. INTRODUCTION

For every prime power q and non-negative integer g , we let $N_q(g)$ denote the maximum number of rational points on a smooth, projective, absolutely irreducible curve of genus g over the finite field \mathbf{F}_q . There are many interesting questions one might ask about the asymptotic rate of growth of $N_q(g)$, but in this paper we will focus on the problem of determining, for specific q and g , reasonably tight upper and lower bounds on $N_q(g)$. In particular, we will consider the case where $g = 4$.

The Riemann Hypothesis for curves over finite fields, proven in the 1940’s by Weil [35–38], shows that for every genus- g curve C over \mathbf{F}_q we have

$$q + 1 - 2g\sqrt{q} \leq \#C(\mathbf{F}_q) \leq q + 1 + 2g\sqrt{q}.$$

This gives the upper bound $N_q(g) \leq q + 1 + 2g\sqrt{q}$. Serre [29] improved this bound for nonsquare q by showing that in fact

$$N_q(g) \leq q + 1 + g\lfloor 2\sqrt{q} \rfloor.$$

When $q \geq 2g + \sqrt{2g} + 1$, this *Weil–Serre upper bound* is usually the best upper bound we know for $N_q(g)$; for certain proper prime powers $q \geq 2g + \sqrt{2g} + 1$ there are improvements that can be made (see, for example, Theorem 4, Proposition 5, and Corollary 6 of [17]), but for primes in this range no such improvements are known.

Date: 14 June 2015.

2010 *Mathematics Subject Classification.* Primary 11G20; Secondary 14G05, 14G10, 14G15.

Key words and phrases. Curve, Jacobian, defect, rational points.

Fifteen years ago, van der Geer and van der Vlugt [10] published a table of the best upper and lower bounds on $N_q(g)$ known at the time, for $g \leq 50$ and for q ranging over small powers of 2 and 3. They regularly updated their tables and posted the updates on van der Geer’s website. Ten years after the first publication of these tables, the website manypoints.org was created by van der Geer, Lauter, Ritzenthaler, and the author (with technical assistance from Geerit Oomens). The [manypoints](http://manypoints.org) tables include results for many more prime powers q than were in [10]: namely, the primes less than 100, the prime powers p^i for $p < 20$ and $i \leq 5$, and the powers of 2 up to 2^7 .

The upper bounds presented in the [manypoints](http://manypoints.org) tables come from a wide variety of sources and techniques, as is explained in the introduction to [18]. But lower bounds for $N_q(g)$ are generally obtained by producing examples of curves with many points, and for most q and g no-one has done thorough searches for such curves.

For $g = 1$, the value of $N_q(g)$ is determined by a result of Deuring [8] (see [34, Theorem 4.1, p. 536]). For $g = 2$, the value of $N_q(g)$ is given by a result of Serre [29–31] (see also [20]). As is explained in [24], there is no easy formula known for $N_q(3)$, but for all q in the [manypoints](http://manypoints.org) tables the value has been computed; the introduction to [26] gives a good summary of the techniques that have been used to find genus-3 curves attaining the maximum number of points.

This leads us to the case $g = 4$. In an earlier paper [16], we obtained new upper and lower bounds on $N_q(4)$ for those prime powers $q < 100$ for which the exact value had not been known. The strategy we used for small q sometimes required us to search through families of curves to determine whether any members of the family had many points. Such strategies do not scale well with the size of the base field.

In this paper, we take a different tack. Instead of performing exhaustive searches to try to find curves with point-counts as close as possible to the Weil–Serre bound, we will exhibit an *efficient* algorithm that we expect will produce curves whose point-counts are *reasonably close* to the Weil–Serre bound. In particular, heuristic arguments suggest that for all sufficiently large primes and for most prime powers q , our Algorithm 6.1 will produce a genus-4 curve over \mathbf{F}_q whose number of points is within 4 of the Weil bound in time $\tilde{O}(q^{3/4})$.

In Section 2 we give Algorithm 2.7, which attempts to produce genus-4 curves over \mathbf{F}_q whose Jacobians split (up to a small isogeny) as a product of a given genus-2 Jacobian and two elliptic curves from a given list. The algorithm takes as input a hyperelliptic curve that can be written $y^2 = f_1 f_2$ for two cubic polynomials f_1 and f_2 , and two lists \mathcal{L}_1 and \mathcal{L}_2 of elliptic curves that are ‘compatible’ (in a sense defined in Section 2) with the polynomials f_1 and f_2 . Heuristically, we expect the algorithm to succeed with probability proportional to $\#\mathcal{L}_1 \#\mathcal{L}_2 / q$, and to run in time linear in $\#\mathcal{L}_1$ and polynomial in $\log q$.

The *defect* of a genus- g curve C over \mathbf{F}_q is the difference between the Weil–Serre bound and the number of points on C :

$$\text{defect } C = (q + 1 + g[2\sqrt{q}]) - \#C(\mathbf{F}_q).$$

In Section 3, we explain how Algorithm 2.7 can be used to produce genus-4 covers D of genus-2 curves C such that the defect of D is not much larger than the defect of C .

In Section 4, which may be of independent interest, we reinterpret some results of Hayashida having to do with principal polarizations on the square of an elliptic curve with complex multiplication. We use these results in Section 5 to show that for many primes q there are many genus-2 curves of small defect over \mathbf{F}_q , and we give an algorithm for finding them.

In Section 6 we put all of the pieces together and present Algorithm 6.1, which, as we noted earlier, can be used to quickly find curves of genus 4 with small defect. In Section 7 we show how Algorithm 6.1 fares in actual practice.

Acknowledgments. The author is grateful to John Voight for sharing a draft of his forthcoming book [33] and for providing the argument involving quaternion algebras that appears in the proof of Theorem 5.8.

2. A FAMILY OF GENUS-4 CURVES COVERING A GENUS-2 CURVE

Let k be a finite field of odd characteristic and let C be a genus-2 curve over k , given by a model $y^2 = f$ where $f \in k[x]$ is a separable polynomial of degree 6. Suppose f can be written $f = f_1 f_2$, where f_1 and f_2 are cubic polynomials. We will associate to this factorization of f a 1-parameter family of genus-4 curves over k that are double covers of C and whose Jacobians are isogenous to the product of the Jacobian of C with two (variable) elliptic curves.

For every $a \in \mathbf{P}^1(k)$ with $a \neq \infty$ and $f(a) \neq 0$, let D_a be the curve defined by the pair of equations

$$\begin{aligned} w^2 &= (x - a)f_1 \\ z^2 &= (x - a)f_2. \end{aligned}$$

For $i = 1$ and $i = 2$ let h_i be the polynomial $x^3 f_i(1/x + a)$ and let $E_{a,i}$ be the elliptic curve $y^2 = h_i$, so that $E_{a,i}$ is isomorphic to the genus-1 curve $y^2 = (x - a)f_i$. To handle the case $a = \infty$, we let D_∞ be the curve defined by $w^2 = f_1, z^2 = f_2$, and for each i we let $E_{\infty,i}$ be the elliptic curve $y^2 = f_i$. If we have call to make the dependence of D_a on f_1 and f_2 explicit, we will write $D_a(f_1, f_2)$.

Theorem 2.1. *For each $a \in \mathbf{P}^1(k)$ such that $f(a) \neq 0$ the curve D_a has genus 4, and there are isogenies*

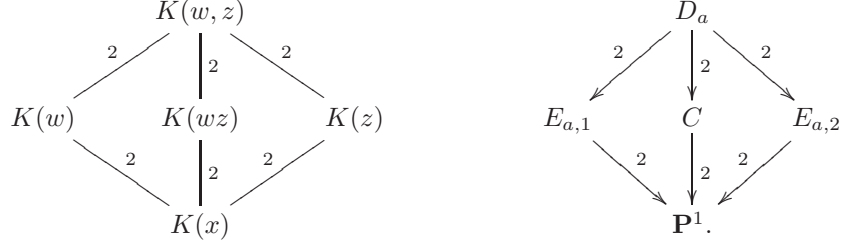
$$\begin{aligned} \varphi: \text{Jac } D_a &\rightarrow (\text{Jac } C) \times E_{a,1} \times E_{a,2} \\ \psi: (\text{Jac } C) \times E_{a,1} \times E_{a,2} &\rightarrow \text{Jac } D_a \end{aligned}$$

such that $\varphi \circ \psi$ and $\psi \circ \varphi$ are multiplication-by-2.

Proof. Let $K = k(x)$, so that the function field of D_a is $K(w, z)$. Since

$$\left(\frac{wz}{x - a} \right)^2 = f_1 f_2 = f,$$

we see that $K(wz/(x-a))$ is isomorphic to the function field of C . The diagram of Galois field extensions on the left then leads to the diagram of curves on the right:



The Galois group of D_a over \mathbf{P}^1 is of course the Klein group V_4 . The images of the pullback maps from $\text{Jac } C$, $E_{a,1}$, and $E_{a,2}$ to $\text{Jac } D_a$ are subvarieties of $\text{Jac } D_a$ that have 0-dimensional pairwise intersections, because a different subgroup of V_4 acts trivially on each of the three subvarieties. Therefore, the three pullback maps piece together to give an isogeny $\psi: (\text{Jac } C) \times E_{a,1} \times E_{a,2} \rightarrow \text{Jac } D_a$, and the pushforwards give an isogeny φ in the other direction. On each factor, the composition $\varphi \circ \psi$ is multiplication by 2, so $\varphi \circ \psi = 2$. The composition in the other order must then also be multiplication by 2. \square

Definition 2.2. Let $f \in k[x]$ be a separable cubic. We say that an elliptic curve E over k is *compatible* with f if E is isomorphic to the curve $y^2 = cf$ for some nonzero $c \in k$ or if E is isomorphic to the curve $y^2 = cx^3f(1/x + a)$ for some $a, c \in k$ with $c \neq 0$.

Lemma 2.3. *An elliptic curve E over k is compatible with a separable cubic $f \in k[x]$ if and only if E and the elliptic curve $y^2 = f$ have the same number of k -rational 2-torsion points.*

Proof. Write E as $y^2 = g$ for some separable cubic g . Then E will have the same number of rational 2-torsion points as $y^2 = f$ if and only if the degrees of the irreducible factors of f and of g are equal. Likewise, these degrees will be equal if and only if there is a linear fractional transformation of \mathbf{P}_k^1 that takes the roots of f to the roots of g .

Suppose there is such a linear fractional transformation. If it is of the form $x \mapsto bx + d$, then E is isomorphic to $y^2 = cf$ for some c . If it is of the form $x \mapsto (bx + d)/(x - a)$, then E is isomorphic to $y^2 = cx^3f(1/x + a)$ for some c .

Conversely, if E is isomorphic to $y^2 = cf$ or $y^2 = cx^3f(1/x + a)$, then clearly the factorization patterns of f and g are equal, so E and the curve $y^2 = f$ have the same number of rational 2-torsion points. \square

Notation 2.4. Let $f \in k[x]$ be a separable cubic. We let $n(f)$ denote the number of automorphisms of \mathbf{P}_k^1 that permute the roots of f .

It is easy to see that $n(f)$ is either 3, 2, or 6, depending on whether f has 0, 1, or 3 rational roots.

Theorem 2.5. *Let C and $f = f_1f_2$ be as above. Let S be the set of roots of f in k , and let T be the set $\{j(E)\}$, where E ranges over all elliptic curves over k compatible with f_1 . The map from $\mathbf{P}^1(k) \setminus S$ to k that sends a to $j(E_{a,1})$ has image contained in T . With at most 5 exceptions, every element of T has exactly $n(f_1)$ preimages; the exceptions have fewer than $n(f_1)$ preimages.*

Proof. The image of the map lies in T by the very definition of compatibility.

Let E be an elliptic curve compatible with f_1 , and suppose $g \in k[x]$ is a cubic polynomial such that E is isomorphic to the curve $y^2 = g$. An element $a \in \mathbf{P}^1(k) \setminus S$ is a preimage for $j(E)$ if and only if there is an automorphism of \mathbf{P}^1 that takes the roots of g to the roots of f_1 and that sends ∞ to a . The number of automorphisms of \mathbf{P}^1 taking the roots of g to the roots of f_1 is equal to $n(f_1)$. These automorphisms will take ∞ to distinct elements of \mathbf{P}^1 unless E has more than 2 automorphisms; that is, unless $j = 0$ or $j = 1728$. These distinct elements will all lie in $\mathbf{P}^1(k) \setminus S$, unless j is the j -invariant of one of the (at most three) curves $y^2 = (x - a)f_1$, for a a root of f_2 . Thus, all but at most five values of j in T will have exactly $n(f_1)$ preimages. \square

Theorem 2.5 says that the j -invariants of the curves $E_{a,1}$ that we get from a given splitting $f = f_1 f_2$ are essentially distributed uniformly at random from among the j -invariants of the elliptic curves over k compatible with f_1 . Also, if a given elliptic curve is obtained as $E_{a,1}$ for a given splitting $f = f_1 f_2$, then its quadratic twist is obtained as $E_{a,1}$ for the *same value of a* from the splitting $f = (cf_1)(f_2/c)$, where c is a nonsquare in k . These observations lead us to the following heuristic.

Heuristic 2.6. *For a given curve C and polynomials f_1, f_2 as above, we will model the pairs $(E_{a,1}, E_{a,2})$ as being chosen uniformly at random from among all pairs (E_1, E_2) of elliptic curves over k compatible with f_1 and f_2 , respectively.*

Now let us use the construction implicit in Theorem 2.1 to create an algorithm for producing genus-4 double covers D_a of a genus-2 curve C , as above, where the curves $E_{a,1}$ and $E_{a,2}$ lie in a prescribed set of elliptic curves.

Algorithm 2.7.

Input: An odd prime power q , coprime cubic polynomials f_1 and f_2 in $\mathbf{F}_q[x]$, and two lists \mathcal{L}_1 and \mathcal{L}_2 of elliptic curves over \mathbf{F}_q compatible with f_1 and f_2 , respectively.

Output: Either the word “failure”, or a value of $a \in \mathbf{P}^1(\mathbf{F}_q)$ such that $f_1(a)f_2(a) \neq 0$ and such that the elliptic curves $E_{a,1}$ and $E_{a,2}$ lie in \mathcal{L}_1 and \mathcal{L}_2 , respectively.

1. Compute the degree-6 rational function $j_1 \in \mathbf{F}_q(t)$ such that the j -invariant of the genus-1 curve $y^2 = (x - a)f_1$ is $j_1(a)$.
2. For every $E_1 \in \mathcal{L}_1$ do:
 - (a) Compute the (at most 6) values $a \in \mathbf{P}^1(\mathbf{F}_q)$ with $j_1(a) = j(E_1)$ and with $f_2(a) \neq 0$.
 - (b) For each of these values, check whether $E_{a,1}$ lies in \mathcal{L}_1 and $E_{a,2}$ lies in \mathcal{L}_2 . If so, output a and stop.
3. Output “failure”.

Note that if there does exist an a such that $E_{a,1}$ and $E_{a,2}$ lie in \mathcal{L}_1 and \mathcal{L}_2 , Algorithm 2.7 will find it. Also, it is clear that there are positive constants c_1 and c_2 such that Algorithm 2.7 runs in probabilistic time at most $c_1 \# \mathcal{L}_1 (\log q)^{c_2}$.

Heuristic Expectation 2.8. *Let q be an odd prime power. Let \mathcal{L}_1 and \mathcal{L}_2 be two nonempty lists of elliptic curves over \mathbf{F}_q such that all the curves in each list have the same number of 2-torsion points, and suppose $\# \mathcal{L}_1 \# \mathcal{L}_2 \ll q^{3/4}$. The*

probability that Algorithm 2.7 will succeed on a randomly chosen pair (f_1, f_2) of cubic polynomials in $\mathbf{F}_q[x]$ compatible with the curves in \mathcal{L}_1 and \mathcal{L}_2 is approximately

$$n(f_1)n(f_2) \frac{\#\mathcal{L}_1 \#\mathcal{L}_2}{4q}.$$

Justification. Using Heuristic 2.6, we view the pairs $(E_{1,a}, E_{2,a})$ as being chosen uniformly at random from among the ordered pairs of elliptic curves compatible with f_1 and f_2 . There are approximately $4q^2/(n(f_1)n(f_2))$ such pairs of compatible curves. The probability that none of the pairs $(E_{1,a}, E_{2,a})$ will lie in the set of $\#\mathcal{L}_1 \#\mathcal{L}_2$ pairs we are hoping to find is then given by

$$\left(1 - n(f_1)n(f_2) \frac{\#\mathcal{L}_1 \#\mathcal{L}_2}{4q^2}\right)^k,$$

where $k \approx q$ is the number of elements of $\mathbf{P}^1(k)$ that are not roots of $f_1 f_2$. Since $\#\mathcal{L}_1 \#\mathcal{L}_2 \ll q^{3/4}$, this probability of failure is approximately

$$1 - n(f_1)n(f_2) \frac{\#\mathcal{L}_1 \#\mathcal{L}_2}{4q},$$

and the probability of success is as stated in the Expectation. \square

3. CHANGE IN DEFECT

Recall that the *defect* of a genus- g curve C over a finite field k is the difference between $\#C(k)$ and the Weil–Serre upper bound for genus- g curves over k . In this section, we consider using Algorithm 2.7 to produce genus-4 curves whose defect is not much more than that of the genus-2 curves that they cover.

Heuristic Expectation 3.1. *Let C be a genus-2 curve over a finite prime field \mathbf{F}_q that can be written in the form $y^2 = f_1 f_2$, where f_1 and f_2 are irreducible cubic polynomials in $\mathbf{F}_q[x]$. Let $m = \lfloor 2\sqrt{q} \rfloor$. If m is even set $k = 1$; if m is odd set $k = 2$. Up to powers of $\log \log q$, the probability that there is a double cover D of C , of the type described in Section 2, such that the defect of D satisfies*

$$\text{defect } D \leq \text{defect } C + 2k$$

is approximately $q^{-1/2}$.

Justification. We start with some comments about the number of elliptic curves with a given small defect. For elliptic curves, the general Weil–Serre bound specializes into the Hasse bound: The maximal number of points on an elliptic curve over \mathbf{F}_q is $q + 1 + m$, where $m = \lfloor 2\sqrt{q} \rfloor$. If m is coprime to q , then there do exist elliptic curves over \mathbf{F}_q with this number of points (see [34, Theorem 4.1, p. 426]). More generally, if t is any integer with $|t| \leq |m|$ and $(t, q) = 1$, then the number of elliptic curves over \mathbf{F}_q with $q + 1 - t$ points is equal to the Kronecker class number $H(t^2 - 4q)$; see [28, Theorem 4.6, pp. 194–195].

Let us consider the number of elliptic curves over \mathbf{F}_q with $q + 1 + m - k$ points, where k is as in the statement of the Expectation. Let $t = k - m$; it is easy to check that when q is prime, t is coprime to q , so the number of elliptic curves of trace t is then equal to the Kronecker class number $H(\Delta)$ of the discriminant $\Delta = t^2 - 4q$. If the Generalized Riemann Hypothesis is true, then up to factors of $\log \log |\Delta|$, this class number is bounded below and above by $\sqrt{|\Delta|}$. (For fundamental discriminants, this is [25, Theorem 1, p. 367], and the result for general discriminants follows easily.)

If we write $m = 2\sqrt{q} - \varepsilon$ with $0 \leq \varepsilon < 1$, then $t = k + \varepsilon - 2\sqrt{q}$ and

$$\Delta = (k + \varepsilon)^2 - 4(k + \varepsilon)\sqrt{q},$$

so certainly $12\sqrt{q} > |\Delta| > \sqrt{q}$. Therefore, assuming GRH, we expect that up to factors of $\log \log q$, the number of elliptic curves with defect k is bounded below and above by $q^{1/4}$.

Now consider applying Algorithm 2.7 to the irreducible cubics f_1 and f_2 , taking the lists \mathcal{L}_1 and \mathcal{L}_2 to both be the set of elliptic curves of defect k . (Note that the value of k is chosen so that the curves of defect k have no rational 2-torsion points, so they are compatible with f_1 and f_2 .)

According to Heuristic Expectation 2.8, we expect the algorithm to succeed with probability $(9/4)(\#\mathcal{L}_1)^2/q$. We have just seen that $\#\mathcal{L}_1 \sim q^{1/4}$, up to factors of $\log \log q$; therefore, we expect success with probability $q^{-1/2}$, up to factors of $\log \log q$. If we have success, then the resulting curve D_a will satisfy

$$d(D_a) = d(C) + d(E_{a,1}) + d(E_{a,2}) = d(C) + 2k. \quad \square$$

We expect a similar result for cubic polynomials f_1 and f_2 with other factorizations. We will only explicitly state one.

Heuristic Expectation 3.2. *Let C be a genus-2 curve over a finite prime field \mathbf{F}_q that can be written in the form $y^2 = f_1 f_2$, where f_1 and f_2 are cubic polynomials in $\mathbf{F}_q[x]$ each with exactly one rational root. Let $m = \lfloor 2\sqrt{q} \rfloor$. If m is even set $k = 2$; if m is odd set $k = 1$. Up to powers of $\log \log q$, the probability that there is a double cover D of C , of the type described in Section 2, such that the defect $d(D)$ of D satisfies*

$$d(D) \leq d(C) + 2k$$

is approximately $q^{-1/2}$.

(Note that, compared to Heuristic Expectation 3.1, the values of k are assigned in the opposite way.)

The justification for this expectation is essentially the same as that for Heuristic Expectation 3.1. The main difference is that now we are considering elliptic curves with even traces and hence even group orders, but we do not want our sets \mathcal{L}_1 and \mathcal{L}_2 to include elliptic curves that have all of their 2-torsion defined over the base field. Fortunately, it is not hard to see (using, for instance, the theory of isogeny volcanoes [9]) that at least half of the curves of trace t do not have all of their 2-torsion points defined over the base field.

4. INTERLUDE ON WORK BY HAYASHIDA

In the late 1960s, Hayashida and Nishi studied genus-2 curves lying on products of isogenous elliptic curves with complex multiplication. Their initial paper [14] studied the general case, and was followed by a paper by Hayashida [13] that considered the special case of curves lying on $E \times E$, for E with CM by a maximal order. In this section we will reinterpret Hayashida's work in terms of an equivalence of categories that is reminiscent of both

- (1) the equivalence of categories between supersingular elliptic curves and rank-1 right modules over a maximal order in a quaternion algebra [23], and

- (2) the bijection between supersingular abelian surfaces (given with an action of a maximal order in a quaternion algebra) and “oriented maximal orders” [27, §3].

First we will define a category of principal polarizations on the square of an elliptic curve. Then we will show that this category is equivalent to the category of rank-1 right modules over an order in a certain quaternion algebra. Finally, we will show that there is an involution on the category such that the orbits of isomorphism classes of objects correspond to “good curves” of genus 2 whose (unpolarized) Jacobian varieties are isomorphic to the square of the given elliptic curve.

4.1. The category of principal polarizations on $E \times E$. Let E be an elliptic curve over an arbitrary field k , let \mathcal{O} be the ring of (k -rational) endomorphisms of E , and suppose that \mathcal{O} is isomorphic to the ring of integers of an imaginary quadratic field K of discriminant Δ . Let A be the abelian surface $E \times E$, and note that the principal polarizations on A are in bijection with the set of positive definite unimodular Hermitian matrices in the matrix ring $M_2(\mathcal{O})$. We denote complex conjugation (in \mathcal{O} and in K) by $x \mapsto \bar{x}$.

Let $P \mapsto P'$ be the involution on $M_2(\mathcal{O})$ that sends a matrix $P = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ to

$$P' = \begin{bmatrix} \bar{d} & -\bar{c} \\ -\bar{b} & \bar{a} \end{bmatrix}.$$

Let $P \mapsto P^*$ denote the conjugate-transpose involution, and note that $P^*P' = (\det P)I$, where I is the identity matrix.

We define a category $\mathcal{Pols} E^2$ as follows: The objects of $\mathcal{Pols} E^2$ are positive definite unimodular Hermitian matrices in $M_2(\mathcal{O})$, that is, principal polarizations on $E \times E$. The set of morphisms from one object L to another object M is defined to be

$$\text{Hom}(L, M) = \{P \in M_2(\mathcal{O}) : MP = P'L\},$$

and composition of morphisms

$$\text{Hom}(M, N) \times \text{Hom}(L, M) \rightarrow \text{Hom}(L, N)$$

is given by sending (Q, P) to QP . It follows that $\mathcal{Pols} E^2$ is a preadditive category. Note that if P is a morphism from L to M , and if we multiply both sides of the equality $MP = P'L$ by P^* , we find that

$$P^*MP = (\overline{\det P})L.$$

Since M and L are both positive definite, we see that $\det P$ must be a non-negative rational integer.

Let I denote the identity matrix in $M_2(\mathcal{O})$. We compute that

$$\text{End } I = \left\{ \begin{bmatrix} \alpha & -\bar{\beta} \\ \beta & \bar{\alpha} \end{bmatrix} : \alpha, \beta \in \mathcal{O} \right\}.$$

Theorem 4.1. *The ring $\text{End } I$ is an order in a quaternion algebra $\mathbf{H} = (\text{End } I) \otimes \mathbf{Q}$ over \mathbf{Q} . The algebra \mathbf{H} is ramified at infinity, at the prime divisors of Δ that are congruent to 3 modulo 4, and at 2 if Δ is even but not congruent to 8 modulo 32. The reduced discriminant of $\text{End } I$ is equal to the discriminant of \mathcal{O} .*

Proof. Set

$$i = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \in \text{End } I,$$

so that $i^2 = -1$. Let $\overline{\mathcal{O}}$ denote the image of \mathcal{O} in $M_2(\mathcal{O})$ under the twisted embedding

$$a \mapsto \begin{bmatrix} a & 0 \\ 0 & \overline{a} \end{bmatrix}.$$

Then $\text{End } I = \overline{\mathcal{O}}[i]$. We write elements of $\overline{\mathcal{O}}[i]$ as $\alpha + i\beta$, with $\alpha, \beta \in \mathcal{O}$, and we note that $\alpha i = i\overline{\alpha}$ for all $\alpha \in \mathcal{O}$. Likewise, we let \overline{K} denote the twisted diagonal image of K in $M_2(K)$, and we note that $\mathbf{H} = \overline{K}[i]$. Clearly \mathbf{H} is a quaternion algebra, and clearly \mathbf{H} is ramified at infinity.

To find the finite primes that ramify in \mathbf{H} , we note that for all $\alpha, \beta \in K$ we have

$$\begin{aligned} (\alpha + i\beta)(\overline{\alpha} - i\beta) &= \alpha\overline{\alpha} + i\beta\overline{\alpha} - \alpha i\beta - i\beta i\beta \\ &= \alpha\overline{\alpha} + i\beta\overline{\alpha} - i\overline{\alpha}\beta - i^2\overline{\beta}\beta \\ &= N(\alpha) + N(\beta), \end{aligned}$$

where N denotes the norm from K to \mathbf{Q} , so a nonzero $\alpha + i\beta$ has norm 0 if and only if $N(\beta) = -N(\alpha)$. Setting $\gamma = \beta/\alpha$, we see that \mathbf{H} is unramified at a prime p if and only if there is an element $\gamma \in K_p = K \otimes \mathbf{Q}_p$ such that $\gamma\overline{\gamma} = -1$.

The norm map from K_p^* to \mathbf{Q}_p^* is surjective on units for all primes p that are unramified in \mathcal{O} , so \mathbf{H} is unramified at these primes. We are left to consider the primes that are ramified in \mathcal{O} ; let p be such a prime.

If $p \equiv 1 \pmod{4}$ then $\mathbf{Z}_p \subset \mathcal{O}_p$ contains an element e whose square is -1 and that is fixed by complex conjugation, so p is unramified in \mathbf{H} . On the other hand, if $p \equiv 3 \pmod{4}$ then no element of K_p has norm -1 , so p is ramified in \mathbf{H} .

This leaves us with the case $p = 2$. We know that $\mathbf{Q}_2^*/\mathbf{Q}_2^{*2}$ is a group of order 8, generated by the images of -1 , 2 , and 3 , and we calculate the following table:

| n | Description of $\mathbf{Q}_2(\sqrt{n})/\mathbf{Q}_2$ | Is -1 a norm in this extension? |
|-----|---|--------------------------------------|
| 1 | split | yes |
| -1 | ramified | no |
| 2 | ramified | yes |
| -2 | ramified | no |
| 3 | ramified | no |
| -3 | unramified | yes |
| 6 | ramified | no |
| -6 | ramified | yes |

We see that \mathbf{H} is ramified at 2 if and only if the 2-adic extension K_2 of \mathbf{Q}_2 is isomorphic to $\mathbf{Q}_2(\sqrt{n})$ with $n = -1, -2, 3$, or 6 . Summarizing, we see that if \mathbf{H} is ramified at 2 then so is K , and if K is ramified at 2 then so is \mathbf{H} , unless the 2-adic extension is isomorphic to $\mathbf{Q}_2(\sqrt{n})$ with $n = 2$ or $n = -6$. This can be summarized even more briefly: if Δ is even, then \mathbf{H} is ramified at 2 unless $\Delta \equiv 8 \pmod{32}$.

Finally, a direct computation shows that the trace dual of $\overline{\mathcal{O}}[i]$ is $\overline{\mathcal{A}}[i]$, where \mathcal{A} is the trace dual of \mathcal{O} . It follows that the reduced discriminant of $\overline{\mathcal{O}}[i]$ is Δ . \square

4.2. An equivalence of categories. We define a functor F from the category $\mathcal{Pols } E^2$ to the category of rank-1 projective right $\overline{\mathcal{O}}[i]$ -modules as follows: If L is a positive definite unimodular matrix, we take $F(L)$ to be the right $(\text{End } I)$ -module $\text{Hom}(I, L)$. If P is a morphism from L to M , we take $F(P)$ to be the morphism

of right $\overline{\mathcal{O}}[i]$ -modules that takes an element Q of $F(L) = \text{Hom}(I, L)$ to the element PQ of $F(M) = \text{Hom}(I, M)$.

Theorem 4.2. *Suppose $\Delta \not\equiv 0 \pmod{8}$. Then the functor F is an equivalence of categories.*

Proof. Before we begin the proof proper, we describe the module $\text{Hom}(I, L)$ a little more concretely. Suppose that $L = \begin{bmatrix} k & \alpha \\ \overline{\alpha} & \ell \end{bmatrix}$ is an element of $M_2(\mathcal{O})$. Let $S = \begin{bmatrix} k & \alpha \\ 0 & 1 \end{bmatrix}$, so that $S^*S = (\det S)L$. By definition,

$$\text{Hom}(I, L) = \{P \in M_2(\mathcal{O}) : LP = P'\}.$$

The condition $LP = P'$ translates into $S^*SP = (\det S)P'$, which is equivalent to $SP = (SP)'$. Since the set of elements $x \in M_2(K)$ satisfying $x = x'$ is exactly $\overline{K}[i]$, this means that

$$\text{Hom}(I, L) = M_2(\mathcal{O}) \cap S^{-1} \cdot \overline{K}[i],$$

where the intersection takes place in $M_2(K)$.

As a right $\overline{\mathcal{O}}[i]$ -module, $\text{Hom}(I, L)$ is isomorphic to

$$S \text{Hom}(I, L) = \left\{ u + iv \in \overline{K}[i] : \begin{bmatrix} 1 & -\alpha \\ 0 & k \end{bmatrix} \begin{bmatrix} u & -\overline{v} \\ v & \overline{u} \end{bmatrix} \in kM_2(\mathcal{O}) \right\}.$$

It is easy to check that this set is generated (as a right \mathcal{O} -module) by the two elements k and $\alpha + i$. Thus, $\text{Hom}(I, L)$ is isomorphic as a right $\overline{\mathcal{O}}[i]$ -module to the ideal $(k, \alpha + i)$. In particular, $\text{Hom}(I, L)$ is a projective rank-1 $\overline{\mathcal{O}}[i]$ -module.

To prove that F gives an equivalence of categories, it suffices to show that F is fully faithful and that F is surjective on isomorphism classes of objects.

Surjectivity: Section 3 of [13] (see in particular the final paragraph) shows that there is a bijection between right $\overline{\mathcal{O}}[i]$ -ideals and what Hayashida calls “proper classes” of unimodular Hermitian matrices. One can check that two unimodular Hermitian matrices are in the same proper class (according to Hayashida’s definition [13, p. 31]) if and only if there are isomorphic in the category $\mathcal{Pols} E^2$. Thus, Hayashida already gives us a bijection between isomorphism classes of objects in $\mathcal{Pols} E^2$ and equivalence classes of right $\overline{\mathcal{O}}[i]$ -ideals.

Full fidelity: Suppose L and M are two objects in $\mathcal{Pols} E^2$, say

$$L = \begin{bmatrix} k & \alpha \\ \overline{\alpha} & \ell \end{bmatrix} \quad \text{and} \quad M = \begin{bmatrix} m & \beta \\ \overline{\beta} & n \end{bmatrix}.$$

Let

$$S = \begin{bmatrix} k & \alpha \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad T = \begin{bmatrix} m & \beta \\ 0 & 1 \end{bmatrix},$$

so that $S^*S = (\det S)L$ and $T^*T = (\det T)M$. By definition, $\text{Hom}(L, M)$ is equal to the set of $P \in M_2(\mathcal{O})$ with $MP = P'L$, and a calculation shows that this last condition is equivalent to $TPS^{-1} = (TPS^{-1})'$. Thus,

$$\text{Hom}(L, M) = M_2(\mathcal{O}) \cap T^{-1} \cdot \overline{K}[i] \cdot S.$$

If P is an element of $\text{Hom}(L, M)$, then the homomorphism $F(P)$ from

$$\text{Hom}(I, L) = M_2(\mathcal{O}) \cap S^{-1} \cdot \overline{K}[i]$$

to

$$\text{Hom}(I, M) = M_2(\mathcal{O}) \cap T^{-1} \cdot \overline{K}[i]$$

is simply multiplication on the left by P .

Now, every morphism from a right $\overline{\mathcal{O}}[i]$ -ideal to another right $\overline{\mathcal{O}}[i]$ -ideal is obtained from left multiplication by an element of $\overline{K}[i]$. In particular, every element of $\text{Hom}(SF(L), TF(M))$ is given by left multiplication by an element of $\overline{K}[i]$, so every element of $\text{Hom}(F(L), F(M))$ is given by left multiplication by an element P of $T^{-1} \cdot \overline{K}[i] \cdot S$. Multiplication by P will take the lattice $M_2(\mathcal{O}) \subset S^{-1} \cdot \overline{K}[i]$ to the lattice $M_2(\mathcal{O}) \subseteq T^{-1} \cdot \overline{K}[i]$ if and only if P lies in $M_2(\mathcal{O})$. Thus, $\text{Hom}(F(L), F(M))$ is also isomorphic to $M_2(\mathcal{O}) \cap T^{-1} \cdot \overline{K}[i] \cdot S$, and the functor F gives one such isomorphism. \square

4.3. An involution on the category of principal polarizations. Set

$$s = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \in M_2(\mathcal{O}),$$

so that $s^2 = I$ and $s' = -s$. We define an involution on $\mathcal{Pols} E^2$ as follows: If L is an object of $\mathcal{Pols} E^2$ we set $\overline{L} = sLs$, and we define an isomorphism $\text{Hom}(L, M) \rightarrow \text{Hom}(\overline{L}, \overline{M})$ by sending $P \in \text{Hom}(L, M)$ to $\overline{P} = sPs$. In this subsection we will define a second category, $\mathcal{Curves} E^2$, whose isomorphism classes of objects correspond to orbits of isomorphism classes of objects of $\mathcal{Pols} E^2$ under this involution.

The objects of $\mathcal{Curves} E^2$ are the same as the objects of $\mathcal{Pols} E^2$: namely, positive definite unimodular Hermitian matrices in $M_2(\mathcal{O})$, which we can also consider to be principal polarizations on $E \times E$. The set of morphisms from one object L to another object M is defined to be

$$\text{Hom}(L, M) = \{P \in M_2(\mathcal{O}) : MP = \pm P'L\};$$

note the plus-or-minus sign in the definition. As in $\mathcal{Pols} E^2$, composition of morphisms

$$\text{Hom}(M, N) \times \text{Hom}(L, M) \rightarrow \text{Hom}(L, N)$$

is given by sending (Q, P) to QP . Unlike $\mathcal{Pols} E^2$, the category $\mathcal{Curves} E^2$ is not preadditive, because if P_1 is an endomorphism of L that takes the plus sign in the definition, and if P_2 is an endomorphism that takes the minus sign, then in general $P_1 + P_2$ will not be an endomorphism of L .

Note that if P is a morphism from L to M , and if we multiply both sides of the equality $MP = \pm P'L$ by P^* , we find that

$$P^*MP = \pm(\overline{\det P})L.$$

Since M and L are both positive definite, we see that $\det P$ is a rational integer. Thus, a morphism from L to M is an element P of $M_2(\mathcal{O})$ such that $\det P$ is a rational integer and such that

$$P^*MP = |\det P|L.$$

Recall that a *good curve of genus 2* is either a nonsingular curve of genus 2 or a pair of elliptic curves crossing transversely at a point. (Over a field that is not algebraically closed, the two elliptic curves may be a Galois conjugate pair of curves defined over a quadratic extension.) For the rest of this section, we will simply write *good curve* when we mean a good curve of genus 2. If C is a good curve consisting of two elliptic curves crossing transversely at a point, its Jacobian is the product of the two elliptic curves, together with the product principal polarization. Torelli's

theorem in genus 2 says that the Jacobian map from the set of good curves to the set of principally-polarized abelian surfaces is a bijection.

Suppose C_1 and C_2 are good curves whose Jacobians are isomorphic to E^2 (as unpolarized surfaces). Let φ_1 and φ_2 be isomorphisms from $\text{Jac } C_1$ and $\text{Jac } C_2$ to E^2 , let λ_1 and λ_2 be the canonical polarizations on $\text{Jac } C_1$ and $\text{Jac } C_2$, let μ be the product principal polarization on E^2 , and for each i let $L_i = \mu^{-1}\varphi_{i*}\lambda_i$, so that $L_i \in M_2(\mathcal{O})$ is a positive definite unimodular Hermitian form.

Note that the good curves C_1 and C_2 are isomorphic to one another if and only if their polarized Jacobians are isomorphic to one another, which will be the case if and only if there is an invertible $P \in M_2(\mathcal{O})$ such that $P^*L_1P = L_2$. If the discriminant Δ of \mathcal{O} is anything other than -3 or -4 , then such an invertible P must have determinant ± 1 , in which case P also gives an isomorphism between L_1 and L_2 in the category *Curves* E^2 . Thus, when $|\Delta| > 4$, the objects of *Curves* E^2 can be viewed as the good curves over k whose Jacobians are isomorphic to E^2 .

5. GENUS-2 CURVES WITH SMALL DEFECT

Given Heuristic Expectations 3.1 and 3.2, our strategy for producing genus-4 curves with small defect is clear: We should try to produce a large number of small-defect curves of genus 2 that can be written $y^2 = f_1f_2$ for cubic polynomials f_1 and f_2 , and then apply Algorithm 2.7 to all of the pairs (f_1, f_2) , taking the sets \mathcal{L}_1 and \mathcal{L}_2 to be the elliptic curves of small defect. As long as we have significantly more than $q^{1/2}$ curves of genus 2 to work with, we should find a small-defect curve of genus 4 in this way.

In this section, we show that in some cases we can prove that there are sufficiently many genus-2 curves of small defect, and we have an efficient way of producing them.

Theorem 5.1. *Let q be a prime power and let t be an integer, coprime to q , with $|t| \leq \lfloor 2\sqrt{q} \rfloor$. Let $\Delta = t^2 - 4q$, write $\Delta = \Delta_0 F^2$ for a fundamental discriminant Δ_0 , and let r be the number of prime factors of Δ_0 . If $|\Delta_0| > 4$ then the number of genus-2 curves over \mathbf{F}_q with Weil polynomial $(x^2 - tx + q)^2$ is at least*

$$\frac{h(\Delta_0)\varphi(|\Delta_0|)}{12 \cdot 2^r},$$

where φ is the Euler φ -function.

In fact, in the case where $|\Delta|$ is prime, we have an exact value for the number of genus-2 curves with the specified Weil polynomial.

Theorem 5.2. *Let q be a prime power and let t be an integer, coprime to q , with $|t| \leq \lfloor 2\sqrt{q} \rfloor$. Let $\Delta = t^2 - 4q$. If $|\Delta|$ is a prime greater than 3, then the number of genus-2 curves over \mathbf{F}_q with Weil polynomial $(x^2 - tx + q)^2$ is exactly $Nh(\Delta)$, where*

$$(1) \quad N = \left\lceil \frac{-\Delta}{24} \right\rceil + \frac{h(\Delta) - 1}{2}.$$

Proof of Theorems 5.1 and 5.2. Suppose we are in the situation of Theorem 5.1, and let E be an elliptic curve over \mathbf{F}_q with trace t and with endomorphism ring of discriminant Δ_0 , that is, with endomorphism ring a maximal order. Hayashida [13, pp. 42–43] gives an exact formula for the number N of nonsingular genus-2 curves whose Jacobians are isomorphic (as unpolarized varieties) to the product $E \times E$; he works over the complex numbers, but the argument works for ordinary elliptic

curves over finite fields as well.¹ The number N depends on Δ in a somewhat complicated way, but for our purposes we need only note two facts. First, if $|\Delta_0| > 4$ then N is at least $\varphi(|\Delta_0|)/24$, and second, when $|\Delta|$ is greater than 3 and is prime (and hence 3 mod 8), Hayashida's formula for N reduces to (1).

How many abelian surfaces with Weil polynomial $(x^2 - tx + q)^2$ can be written as $E \times E$, where E has CM by a maximal order? The set of E with CM by Δ_0 is in bijection with the class group of Δ_0 , and two such curves E_1 and E_2 have isomorphic squares if and only if their associated ideal classes have squares that are equal. Thus, the set of surfaces of the form $E \times E$ where E has CM by Δ_0 is in bijection with the set of squares in the class group. Since the 2-rank of the class group is $r - 1$, there are $h(\Delta_0)/2^{r-1}$ such surfaces. Combining this equality with the lower bound on N from the proceeding paragraph gives us the lower bound of Theorem 5.1.

When $-\Delta$ is prime we have $\Delta_0 = \Delta$, and every element of the class group is a square. Thus, there are exactly $Nh(\Delta)$ curves over \mathbf{F}_q with the given Weil polynomial, as claimed in Theorem 5.2. \square

Theorems 5.1 and 5.2 include a requirement that t be coprime to q . We will see similar conditions frequently enough in what follows to justify the following definition.

Definition 5.3. Let d be a non-negative integer. A prime power q is *d-exceptional* if there are no elliptic curves of defect d over the finite field \mathbf{F}_q ; otherwise, q is *d-unexceptional*.

For positive d and for q that are not too small, it is easy to tell when q is d -exceptional.

Proposition 5.4. Let d be a positive integer and let q be a prime power with $q > 56d^2$. Then q is d -exceptional if and only if q is not coprime to $\lfloor 2\sqrt{q} \rfloor - d$.

Proof. Let $t = \lfloor 2\sqrt{q} \rfloor - d$. If $q > 56d^2$ then t certainly lies in the Weil interval, and according to [28, Theorem 4.2, p. 193] there will exist elliptic curves over \mathbf{F}_q with trace t if and only if either t is coprime to q or t is not coprime to q and lies in a short list of possible values. The defects associated to these possible values are 0 (if q is a square) and possibly several other values, all of which are at least $(2 - \sqrt{3})\sqrt{q} - 1$. Since $q > 56d^2$, if q is d -unexceptional then d is one of these values and we have

$$d \geq (2 - \sqrt{3})\sqrt{q} - 1 > (2 - \sqrt{3})\sqrt{56}d - 1 > 2d - 1,$$

which is impossible. Therefore, there are elliptic curves over \mathbf{F}_q of defect d if and only if $\lfloor \sqrt{2q} \rfloor - d$ is coprime to q . \square

Corollary 5.5. Let d be a positive integer and let q be a prime power with $q > 56d^2$. If q is prime, or if q is a square that is coprime to d , then q is d -unexceptional. \square

Heuristically, for every fixed $d > 0$ one expects the number of d -exceptional primes powers less than x to grow like a constant times $\log x$.

¹ Note that there is a misprint on page 43 of [13]: The term $(1/4)(1 - (-1))^{(m^2-1)/8}$ in the second line should be $(1/4)(1 - (-1)^{(m^2-1)/8})h$.

In Theorem 5.1, if q is coprime to t and if the conductor F is equal to 1, then the theorem leads to a lower bound of

$$\frac{h(\Delta)\varphi(|\Delta|)}{12 \cdot 2^r} \geq \frac{h(\Delta)\varphi(|\Delta|)}{12 \cdot \mathcal{D}(|\Delta|)}$$

for the number of genus-2 curves with the specified Weil polynomial, where \mathcal{D} is the divisor function. We know that there is a constant c such that $\varphi(n) > cn/\log n$ for all n (see [12, Theorem 328, p. 267]), and we know that under the GRH we have $h(\Delta) > c'\sqrt{|\Delta|}/\log \log |\Delta|$ for some constant c' (see [25, Theorem 1, p. 367]). Furthermore, the divisor function $\mathcal{D}(n)$ has average order $\log n$ and normal order $(\log n)^{\log 2}$ (see [12, Theorem 319, p. 264] and [12, Theorem 432, p. 359]). In the case where we are considering the squares of isogeny classes of elliptic curves with small positive defect d , we have $\Delta \approx d\sqrt{q}$, and we are led to suggest the following heuristic.

Heuristic 5.6. *For every prime q and integer $d \geq 0$, let $M_{q,d}$ be the number of genus-2 curves over \mathbf{F}_q with Jacobians isogenous to the square of an elliptic curve with defect d . For each fixed $d > 0$, we will model $M_{q,d}$ as growing like $q^{3/4}$, up to logarithmic factors, as q ranges over the prime powers that are d -unexceptional.*

Note that when $d = 0$ we would still expect $M_{q,d}$ to be $\tilde{O}(q^{3/4})$, but we do not expect a lower bound of the same shape — indeed, if q is a prime of the form $n^2 + 1$, then $M_{q,0} = 0$.

Heuristic 5.6 suggests that there are relatively many genus-2 curves with small defect. For the purpose of constructing examples, though, we need more than a simple statement of existence; we would like a way of *producing* these curves of small defect. Here is an algorithm that in certain cases is guaranteed to do so.

Algorithm 5.7.

Input: An odd prime power q and a list \mathcal{L} of elliptic curves over \mathbf{F}_q with defect at most d .

Output: A list of genus-2 curves over \mathbf{F}_q with defect at most $2d$.

1. Initialize S to be the empty list.
2. For every pair of elliptic curves E_1, E_2 in \mathcal{L} :
 - (a) Use Algorithm 5.1 (pp. 183–184) of [5] to compute the set of genus-2 curves over \mathbf{F}_q whose Jacobians are $(2, 2)$ -isogenous to $E_1 \times E_2$.
 - (b) Append to S all of the resulting curves that are not already isomorphic to a curve in S .
3. Set $i = 1$.
4. Repeat the following until $i > \#S$:
 - (a) Let C be the i -th element of S .
 - (b) Compute all of the genus-2 curves over \mathbf{F}_q that are Richelot isogenous to C , using the formulas from [6, §4].
 - (c) Append to S all of the resulting curves that are not already isomorphic to a curve in S .
 - (d) Increment i .
5. Output S .

Theorem 5.8. *Let q be an odd prime power, let $d \geq 0$ be an integer, let $t = \lfloor 2\sqrt{q} \rfloor - d$, and suppose t is odd, positive, and coprime to q . Let $\Delta = t^2 - 4q$, and write $\Delta = \Delta_0 F^2$ for a fundamental discriminant Δ_0 . Let S be the list produced by Algorithm 5.7 given q and the list of defect- d elliptic curves over \mathbf{F}_q as input. Suppose that the exponent of the class group of Δ_0 is greater than 2. Then S contains all genus-2 curves C over \mathbf{F}_q such that the Jacobian of C is isomorphic (as an unpolarized abelian surface) to the square of an elliptic curve with defect d and with CM by Δ_0 .*

Note that there are at most 66 negative fundamental discriminants whose class groups have exponent at most 2, and there are exactly 65 such discriminants if the GRH is true, the largest in absolute value being -5460 [39, Theorem 1, p. 119]. A list of these 65 discriminants is given in [3, Table 5.1, p. 426].

Proof of Theorem 5.8. Recall that a Richelot isogeny from a genus-2 curve C is obtained by taking a subgroup-scheme G of $(\text{Jac } C)[2]$ that is maximal isotropic with respect to the Weil pairing and observing that the quotient variety $A = (\text{Jac } C)/G$ has a natural principal polarization λ such that the pullback of λ to $\text{Jac } C$ is twice the canonical principal polarization on $\text{Jac } C$. When the principally-polarized surface (A, λ) is the Jacobian of a curve D , we say that we have a Richelot isogeny from C to D (or from $\text{Jac } C$ to $\text{Jac } D$). But (A, λ) might also *not* be a Jacobian; it might be the product of two elliptic curves with the product polarization.² This is precisely the situation discussed in [19, §3]. One could continue to say (A, λ) is the Jacobian of a curve — the *singular* genus-2 curve consisting of the union of the two elliptic curves, crossing transversely at their origins. We will use the term “generalized Richelot isogeny” to refer to this slightly expanded concept; however, we should keep in mind that Algorithm 5.7 refers only to Richelot isogenies between nonsingular genus-2 curves.

Let \mathcal{O} be the imaginary quadratic order of discriminant Δ_0 . We note that $\Delta \equiv 5 \pmod{8}$, so we also have $\Delta_0 \equiv 5 \pmod{8}$, so that 2 is inert in \mathcal{O} , and the only simple \mathcal{O} -module of 2-power order is $\mathcal{O}/2\mathcal{O}$. Let E be an elliptic curve with trace t and with CM by \mathcal{O} . The elliptic curves isogenous to E with CM by \mathcal{O} form a principal homogeneous space for the class group $\text{Cl } \mathcal{O}$ of \mathcal{O} ; we choose E to be a base point for the action of the class group. Finitely generated torsion-free \mathcal{O} -modules are determined by their rank and their Steinitz class; as a consequence, if E_1, E_2, E_3 , and E_4 are elliptic curves corresponding to elements g_1, g_2, g_3 , and g_4 of $\text{Cl } \mathcal{O}$, then the surfaces $E_1 \times E_2$ and $E_3 \times E_4$ are isomorphic if and only if $g_1 + g_2 = g_3 + g_4$. If A is an abelian surface isogenous to $E \times E$ with Frobenius endomorphism π such that $\mathbf{Q}(\pi) \cap \text{End } A \cong \mathcal{O}$, then A is isomorphic to $E_1 \times E_2$ for two elliptic curves with CM by \mathcal{O} , which themselves correspond as above to two element g_1 and g_2 of the class group $\text{Cl } \mathcal{O}$; the *Steinitz class* of A (with respect to the base point E) is the element $g_1 + g_2$ of $\text{Cl } \mathcal{O}$.

Let g be an element of $\text{Cl } \mathcal{O}$ that is not 2-torsion, and let E_1 and E_2 be the elliptic curves corresponding to g and to $-g$, so that E_1 and E_2 are not isomorphic to one another. Let $P_1 \in E_1[2](\overline{\mathbf{F}}_q)$ and $P_2 \in E_2[2](\overline{\mathbf{F}}_q)$ be generators for the simple \mathcal{O} -modules $E_1[2](\overline{\mathbf{F}}_q)$ and $E_2[2](\overline{\mathbf{F}}_q)$, and let $\psi: E_1[2](\overline{\mathbf{F}}_q) \rightarrow E_2[2](\overline{\mathbf{F}}_q)$ be

² *A priori*, it might also be the Weil restriction of a polarized elliptic curve over \mathbf{F}_{q^2} [11, Theorem 3.1, p. 270], but no such Weil restriction is isogenous to the square of an elliptic curve with nonzero trace.

the unique \mathcal{O} -module isomorphism that sends P_1 to P_2 . Then the construction of [19, Proposition 4, p. 324], applied to E_1 , E_2 , and ψ , will produce a genus-2 curve C whose Jacobian J is isomorphic to $E_1 \times E_2$ divided by the graph X of ψ . The ring \mathcal{O} acts on X , so \mathcal{O} acts on J compatibly with Frobenius, so J has a Steinitz class. The class of the \mathcal{O} -module X in the class group is trivial, so the Steinitz class of J is equal to that of $E_1 \times E_2$, which is trivial; therefore J is isomorphic to E^2 . The curve C is included in the output of Algorithm 5.1 of [5], applied to E_1 and E_2 . This shows that after step 2, the set S from Algorithm 5.7 includes at least one curve C whose Jacobian is isomorphic (as an unpolarized surface) to E^2 . Let D be any other curve over \mathbf{F}_q whose Jacobian is isomorphic to E^2 . We will show that there is a sequence of generalized Richelot isogenies starting from $\text{Jac } C$ and ending at $\text{Jac } D$. To prove this, we will work with the category $\mathcal{Pols } E^2$ discussed in Section 4.

The quaternion algebra \mathbf{H} associated in Section 4 to $\mathcal{Pols } E^2$ is the quaternion algebra over \mathbf{Q} ramified at ∞ and at the prime divisors of Δ_0 that are congruent to 3 modulo 4, and the order $\overline{\mathcal{O}}[i]$ of \mathbf{H} defined in Section 4 has discriminant equal to the squarefree integer Δ_0 . It follows from [1, Proposition 1.54, p. 12] that $\overline{\mathcal{O}}[i]$ is an Eichler order in \mathbf{H} of level equal to the product of the prime divisors of Δ_0 that are congruent to 1 modulo 4.

Let L and M be principal polarizations on E^2 such that (E^2, L) and (E^2, M) are isomorphic to $\text{Jac } C$ and $\text{Jac } D$ as principally-polarized surfaces, and let I and J be the right ideal classes of $\overline{\mathcal{O}}[i]$ corresponding to L and M under the equivalence of categories described in Section 4. We claim that there is an element α of \mathbf{H} such that $\alpha I \subseteq J$ and such that the index of αI in J is a power of 2. To see this, we use the following result, found in the section of [33] devoted to applications of the strong approximation theorem (paraphrased here with slightly different notation):

Let \mathbf{H} be a definite quaternion algebra over a totally real field F with ring of integers R , and let O be an R -order in \mathbf{H} such that for all finite primes \mathfrak{p} of R , the local norm maps $O_{\mathfrak{p}}^* \rightarrow R_{\mathfrak{p}}^*$ are surjective. Suppose the narrow class group of R is trivial, and let \mathfrak{p} be a prime of R which is unramified in \mathbf{H} . Then every ideal class of O contains an integral O -ideal whose reduced norm is a power of \mathfrak{p} .

Our order $\overline{\mathcal{O}}[i]$ is an Eichler order, so the condition on the local norm maps is satisfied for all primes p of \mathbf{Z} . Also, 2 is unramified in \mathbf{H} .

The ideal J is invertible because the order $\overline{\mathcal{O}}[i]$ is hereditary (because its reduced discriminant is squarefree). Consider the right order O of the lattice IJ^{-1} ; it is locally isomorphic to $\overline{\mathcal{O}}[i]$ at every prime, so it also satisfies the condition on norm maps given above. Applying the quoted result with $\mathfrak{p} = 2$, we find that there is an $\alpha \in \mathbf{H}$ such that αIJ^{-1} is an integral ideal of norm 2^i for some $i > 0$. In particular, $\alpha I \subseteq J$, and the index of αI in J is a power of 2.

Translating this back into the category $\mathcal{Pols } E^2$, we find that there is a $P \in \text{Hom}(L, M)$ of determinant 2^i such that

$$P^*MP = (\overline{\det P})L.$$

In terms of abelian surfaces, this means that we have an isogeny φ of degree 2^i from $\text{Jac } C$ to $\text{Jac } D$ such that the pullback φ^*M of the principal polarization on

$\text{Jac } D$ is equal to 2^i times the polarization L . We will show that φ can be written as a composition of generalized Richelot isogenies.

We note that the kernel of φ is a maximal isotropic subgroup of the 2^i -torsion of $\text{Jac } C$. Now there are two possibilities: Either $(\ker \varphi) \cap (\text{Jac } C)[2]$ is all of $(\text{Jac } C)[2]$, or it is an order-4 subgroup.

Suppose $(\ker \varphi) \cap (\text{Jac } C)[2] = (\text{Jac } C)[2]$. Note that $(\text{Jac } C)[2](\overline{\mathbf{F}}_q)$ is a vector space over $k := \mathcal{O}/2\mathcal{O} \cong \mathbf{F}_4$, and the Weil pairing on $(\text{Jac } C)[2]$ is *semi-balanced* with respect to this action of k ; that is, we have $e_2(\alpha P, Q) = e_2(P, \overline{\alpha} Q)$ for every $P, Q \in (\text{Jac } C)[2](\overline{\mathbf{F}}_q)$ and $\alpha \in k$, where $\overline{\alpha}$ is the conjugate of α over \mathbf{F}_2 . Then [15, Lemma 7.3, p. 2378] shows that there is a one-dimensional isotropic k -subspace G of $(\text{Jac } C)[2]$. The group G is a maximal isotropic subgroup of $(\text{Jac } C)[2]$, so we obtain a generalized Richelot isogeny whose kernel is contained in the kernel of φ . In other words, φ factors through a generalized Richelot isogeny.

On the other hand, suppose $(\ker \varphi) \cap (\text{Jac } C)[2]$ has order 4. Then $(\ker \varphi)(\overline{\mathbf{F}}_q)$ is isomorphic as an abelian group to $\mathbf{Z}/2^i\mathbf{Z} \times \mathbf{Z}/2^i\mathbf{Z}$. Let P and Q be generators of $(\ker \varphi)(\overline{\mathbf{F}}_q)$. Since $\ker \varphi$ is an isotropic subgroup of $(\text{Jac } C)[2^i]$, we have $e_{2^i}(P, Q) = 1$, where e_{2^i} is the Weil pairing on $(\text{Jac } C)[2^i]$. From the compatibility of the Weil pairing, it follows that $e_2(2^{i-1}P, 2^{i-1}Q) = 1$. Let $G = (\ker \varphi) \cap (\text{Jac } C)[2]$, so that $G(\overline{\mathbf{F}}_q)$ is generated by $2^{i-1}P$ and $2^{i-1}Q$. We see that G is a maximal isotropic subgroup of $(\text{Jac } C)[2]$, and arguing as in the preceding paragraph, we find that φ factors through a generalized Richelot isogeny.

In either case, φ factors through a generalized Richelot isogeny. Repeating this argument, we find that φ is in fact a composition of generalized Richelot isogenies.

This almost, but not quite, shows that after Step 4 the set S from Algorithm 5.7 contains all curves whose Jacobians are isomorphic (as unpolarized surfaces) to E^2 . The lacuna in the argument is that the sequence of generalized Richelot isogenies from (E^2, L) to (E^2, M) may pass through singular curves, as discussed above. Suppose this is the case, and consider the split polarized surface $E_1 \times E_2$ closest to (E^2, M) along the given path of generalized Richelot isogenies. The first surface *after* $E_1 \times E_2$ will be a genus-2 curve obtained via the Howe–Leprévost–Poonen construction [19, Proposition 4, p. 324], and so will appear in the set S after step 2. The path of generalized Richelot isogenies from $E_1 \times E_2$ to (E^2, M) does *not* contain any further split polarized surfaces, so by the end of step 4, the set S constructed by Algorithm 5.7 will contain (E^2, M) . \square

Remark 5.9. In practice it can be helpful to modify Step 2(a) of Algorithm 5.7. In addition seeding the list S with curves whose Jacobians are $(2, 2)$ -isogenous to products of two elliptic curves of defect d , we can also throw in curves whose Jacobians are $(3, 3)$ -isogenous to a product of such elliptic curves, by using Algorithm 5.4 (p. 185) of [5].

Heuristic Expectation 5.10. Fix $d \geq 0$. As q varies over the odd prime powers, Algorithm 5.7, applied to q and the list of trace- d elliptic curves over \mathbf{F}_q , runs in time $\tilde{O}(q^{3/4})$. Furthermore, if $d > 0$ and q is d -unexceptional, the algorithm produces $q^{3/4}$ curves, up to logarithmic factors.

Justification. For a fixed d , Heuristic 5.6 suggests that the number of curves produced by the algorithm is bounded above by $q^{3/4}$, up to logarithmic factors. When $d > 0$ and q is d -unexceptional, we expect the number of curves is bounded below

by a similar expression. The time taken by the algorithm is the size of its output, times factors of $\log q$. \square

6. GENUS-4 CURVES WITH SMALL DEFECT

In this section we present our algorithm for producing genus-4 curves with small defect.

Algorithm 6.1.

Input: An odd prime power $q = p^e$.

Output: A genus-4 curve over \mathbf{F}_q , or the word “failure”.

1. Compute $m = \lfloor 2\sqrt{q} \rfloor$, set $d = 0$, and set $\mathcal{L} = \{\}$.
2. Set $t = d - m$. If $p \mid t$, then skip to Step 10.
3. Set $\Delta = t^2 - 4q$ and write $\Delta = \Delta_0 F^2$ for a fundamental discriminant Δ_0 .
4. Using the algorithm of [32], compute the mod- q reductions of the Hilbert class polynomials of discriminant $\Delta_0 f^2$ for all divisors f of F .
5. Compute the roots in \mathbf{F}_q of these Hilbert class polynomials.
6. Compute representatives of all of the isomorphism classes of elliptic curves whose j -invariants are among these roots, and let \mathcal{E}_d be the subset of those elliptic curves whose defect is d .
7. Add the elements of \mathcal{E}_d to the set \mathcal{L} .
8. Run Algorithm 5.7 with inputs q and \mathcal{L} .
9. For each curve C in the output of Algorithm 5.7:
 - (a) Write C as $y^2 = f$ for a sextic polynomial f .
 - (b) For each factorization of f into a pair f_1, f_2 of cubics (up to order and up to scaling by squares in \mathbf{F}_q), run Algorithm 2.7 on $q, f_1, f_2, \mathcal{L}_1$, and \mathcal{L}_2 , where each \mathcal{L}_i is the set of curves in \mathcal{L} that are compatible with f_i .
 - (c) If Algorithm 2.7 outputs an element $a \in \mathbf{P}^1(\mathbf{F}_q)$, output the curve $D_a(f_1, f_2)$ from Section 2 and stop.
10. Increment d . If $d > m$, output “failure” and stop. Otherwise, go to step 2.

Remark 6.2. In Step 2 we avoid the case $p \mid t$ solely to make the analysis of the algorithm simpler. In actual practice, we will encounter the case $p \mid t$ most often when q is a square and $d = 0$. In this case, we should simply compute the set \mathcal{E}_d of (supersingular) elliptic curves of defect 0 in any of a number of ways — by using the formulas from [21], for example, or by using the algorithm of Bröker [4] to compute one such curve and then computing the graph of 2-isogenies — and then continue with Step 7.

Heuristic Expectation 6.3. *For large odd 1-unexceptional prime powers q , Algorithm 6.1 will output a curve of defect at most 4 in time $\tilde{O}(q^{3/4})$.*

The justification of this heuristic expectation depends on knowing something about the Galois structure of the Weierstrass points of the genus-2 curves produced by Algorithm 5.7; we need to know that some fraction of these curves can be used in Algorithm 2.7. Proposition 6.4 below gives us the information we need. Let us begin by setting up the notation for the proposition.

Let E be an ordinary elliptic curve over a finite field \mathbf{F}_q of odd characteristic and let π be the Frobenius endomorphism of E . Let R be the subring $\mathbf{Z}[\pi]$ of

End E . From [7] we know that the abelian surfaces isogenous to E^2 are in bijection with the torsion-free R -modules of rank 2, and results of Borevič and Faddeev [2] (summarized in [22, Theorem 48, p. 326]) classify such R -modules. Pushing this classification back through Deligne's result, we find the following: Every abelian surface A isogenous to E^2 can be written as $E_1 \times E_2$ for two elliptic curves with $\text{End } E_1 \supseteq \text{End } E_2$; if A can also be written $E'_1 \times E'_2$ where $\text{End } E'_1 \supseteq \text{End } E'_2$, then $\text{End } E'_1 \cong \text{End } E_1$ and $\text{End } E'_2 \cong \text{End } E_2$; and, given any elliptic curve E'_1 with $\text{End } E'_1 \cong \text{End } E_1$, there is a unique E'_2 such that $A \cong E'_1 \times E'_2$.

Suppose A is isogenous to E^2 , and write $A \cong E_1 \times E_2$ as above. Note that the conductor of the quadratic order $\text{End } E_1$ divides that of $\text{End } E_2$; it follows that the dimension d_1 of the \mathbf{F}_2 -vector space $E_1[2](\mathbf{F}_q)$ is greater than or equal to the dimension d_2 of $E_2[2](\mathbf{F}_q)$. Also, since $E_1(\mathbf{F}_q)$ has even order if and only if $E_2(\mathbf{F}_q)$ has even order, we have $d_1 = 0$ if and only if $d_2 = 0$.

Proposition 6.4. *With notation as above, let \mathcal{C} be the isogeny class of E and let \mathcal{S} be the set of genus-2 curves over \mathbf{F}_q whose Jacobians are isomorphic (as unpolarized surfaces) to A .*

- (1) *If $(d_1, d_2) = (0, 0)$, then every curve in \mathcal{S} can be written in the form $y^2 = f_1 f_2$ for irreducible cubic polynomials $f_1, f_2 \in \mathbf{F}_q[x]$, and every curve in \mathcal{C} is compatible with both f_1 and f_2 .*
- (2) *If $(d_1, d_2) = (2, 2)$, then every curve in \mathcal{S} can be written in the form $y^2 = f_1 f_2$ for cubic polynomials $f_1, f_2 \in \mathbf{F}_q[x]$ that are completely split, and at least $1/4$ of the curves in \mathcal{C} are compatible with both f_1 and f_2 .*
- (3) *If $(d_1, d_2) = (2, 1)$, then every curve in \mathcal{S} can be written in the form $y^2 = f_1 f_2$ for cubic polynomials $f_1, f_2 \in \mathbf{F}_q[x]$, where f_1 has only one root and f_2 is completely split; at least $1/2$ of the curves in \mathcal{C} are compatible with f_1 , and at least $1/4$ are compatible with f_2 .*
- (4) *Suppose $(d_1, d_2) = (1, 1)$. If C is a curve in \mathcal{S} , then C can either be written in the form $y^2 = f_1 f_2 f_3$ for three irreducible quadratic polynomials $f_1, f_2, f_3 \in \mathbf{F}_q[x]$, or in the form $y^2 = f_1 f_2$, where f_1 and f_2 are cubic polynomials, each with exactly one root. At least $1/4$ of the curves in \mathcal{S} are of the latter type; and, for these curves, at least $1/2$ of the curves in \mathcal{C} are compatible with both f_1 and f_2 .*

Proof. We note for future reference that if the curves in \mathcal{C} have even group orders, then the theory of isogeny volcanoes shows that either no curves in \mathcal{C} have 2-rank equal to 2, or at least $1/4$ of them do. Similarly, at least $1/2$ of the curves in \mathcal{C} have 2-rank equal to 1.

Suppose C is a curve in \mathcal{S} . The six Weierstrass points of C fall into orbits under the action of the absolute Galois group of \mathbf{F}_q , and the orbit structure determines the ranks of the 2-torsion subgroup of $\text{Jac } C$ over the extensions of \mathbf{F}_q . These ranks are also determined by the pair (d_1, d_2) . Comparing these ranks (for the first three extensions of \mathbf{F}_q) for the various possible Galois structures and the various possible pairs (d_1, d_2) , we find the following:

The only Galois orbit structure compatible with $(d_1, d_2) = (0, 0)$ is for the Weierstrass points to be divided into two orbits of size 3; this translates into C being of the form $y^2 = f_1 f_2$ for two irreducible cubics f_1 and f_2 . The curves in \mathcal{C} have no rational points of order 2, so f_1 and f_2 are compatible with all of the curves in \mathcal{C} .

Similarly, the only Galois orbit structure that is compatible with $(d_1, d_2) = (2, 2)$ is six orbits of size 1; this means that C can be written (in several ways) as $y^2 =$

$f_1 f_2$, for two completely split cubics f_1 and f_2 . Since E_1 and E_2 both have 2-rank equal to 2, we see that at least $1/4$ of the curves in \mathcal{C} have 2-rank equal to 2, and each such curve is compatible with both f_1 and f_2 .

The only Galois orbit structure compatible with $(d_1, d_2) = (2, 1)$ is one orbit of size 2 and four of size 1; this means that C can be written (in several ways) as $y^2 = f_1 f_2$, where f_1 is a cubic with only one root and f_2 is a completely split cubic. At least $1/2$ of the curves in \mathcal{C} have 2-rank equal to 1 and are compatible with f_1 ; and, since E_1 has 2-rank equal to 2, at least $1/4$ of the curves in \mathcal{C} have 2-rank equal to 2 and are compatible with f_2 .

We are left to consider the case $(d_1, d_2) = (1, 1)$. There are two Galois orbit structures compatible with these values of d_1 and d_2 : three orbits of size 2, or two orbits of size 2 and two of size 1. To analyze this case, we consider a graph G constructed as follows.

We let the vertices of G be the isomorphism classes of principal polarizations on A . Given two principal polarizations λ and μ , we connect the associated vertices with an edge if and only if there is a diagram

$$(2) \quad \begin{array}{ccc} A & \xrightarrow{2\lambda} & \hat{A} \\ \Phi \downarrow & & \uparrow \hat{\Phi} \\ A & \xrightarrow{\mu} & \hat{A} \end{array}$$

Each edge from a vertex λ gives rise to a Galois-stable subgroup of $A[2](\overline{\mathbf{F}}_q)$ that is maximal isotropic with respect to the Weil pairing associated to λ — namely, $\ker \Phi$.

Let us call a polarization λ of A *bad* if the polarized variety (A, λ) is isomorphic to the Jacobian of a curve C whose Weierstrass points form three Galois orbits of size 2; *good* if the polarized variety (A, λ) is isomorphic to the Jacobian of a curve C whose Weierstrass points form two Galois orbits of size 2 and two of size 1; and *split* if the polarized variety (A, λ) is isomorphic to the product of two elliptic curves with the corresponding product polarization. We will show that in the graph G , every bad vertex is adjacent to at least one good vertex, and every good vertex is connected to at most three bad vertices. From this it follows that there are at most three times as many bad polarizations as good ones, and therefore at least $1/4$ of the curves in \mathcal{S} can be written $y^2 = f_1 f_2$ for cubics f_1 and f_2 , each with exactly one root.

Any morphism from A to its dual variety that is equal to its own dual morphism can be represented by a 2×2 array

$$L = \begin{bmatrix} k & \overline{\alpha} \\ \alpha & \ell \end{bmatrix},$$

where k and ℓ are integers, α is a homomorphism from E_1 to E_2 , and $\overline{\alpha}$ is the dual morphism from E_2 to E_1 . Such an array gives an endomorphism of $E_1 \times E_2$; composed with the product polarization from $E_1 \times E_2$ to its dual, this endomorphism gives a polarization if k , ℓ , and $k\ell - \deg \alpha$ are all positive, and a principal polarization if $k\ell - \deg \alpha = 1$.

We will show that a polarization is bad if and only if the array associated to it has k and ℓ both even. To do this, we will count the number of Galois-stable subgroups of $A[2](\overline{\mathbf{F}}_q)$ that are maximal isotropic subgroups with respect to the Weil pairing

induced by the polarization. First we count the number of such subgroups for good, bad, and split curves, and then we count these subgroups for polarizations of A given by arrays as above.

Suppose λ is a bad polarization, corresponding to a curve C . The Galois-stable maximal isotropic subgroups of $(\text{Jac } C)[2](\overline{\mathbf{F}}_q)$ correspond to Galois-stable partitions of the six Weierstrass points of C into three disjoint subsets of size two. For a bad curve, it is easy to check that there are seven such partitions.

Similarly, if λ is a good polarization, we find that there are exactly three Galois-stable maximal isotropic subgroups of the 2-torsion. If λ is a split polarization, then again there are exactly three such subgroups. This shows that good curves and split curves are connected to at most three other vertices in the graph G , and in particular are connected to at most three bad vertices.

Now let us count the Galois-stable subgroups of $A[2](\overline{\mathbf{F}}_q)$ that are maximal isotropic with respect to the Weil pairing obtained from a polarization described by an array as above. First we simply count the Galois-stable subgroups of order four, *without* the isotropy condition.

For each i let P_i be the rational 2-torsion point of E_i and let Q_i be a non-rational 2-torsion point of E_i . Note that $A[2](\overline{\mathbf{F}}_q)$ contains exactly seven Galois-stable subgroups of order 4, namely:

$$(3) \quad \begin{aligned} &\langle (P_1, 0), (Q_1, 0) \rangle, \quad \langle (0, P_2), (0, Q_1) \rangle, \\ &\quad \langle (P_1, 0), (Q_1, P_2) \rangle, \quad \langle (0, P_2), (P_1, Q_2) \rangle, \quad \langle (P_1, P_2), (Q_1, Q_2) \rangle, \\ &\quad \langle (P_1, P_2), (Q_1, Q_2 + P_2) \rangle, \quad \langle (P_1, 0), (0, P_2) \rangle. \end{aligned}$$

We check that all seven of these subgroups are isotropic with respect to the Weil pairing on the 2-torsion associated to a polarization λ if and only if the array L associated to λ has k and ℓ both even. Thus, the bad polarizations are precisely the polarization that can be represented by endomorphisms

$$L = \begin{bmatrix} k & \overline{\alpha} \\ \alpha & \ell \end{bmatrix}$$

such that both k and ℓ are even.

Suppose λ is bad, represented by an L as above with k and ℓ even. First, we will show that there is a polarization isomorphic to λ whose associated L has $k \equiv 2 \pmod{4}$ or $\ell \equiv 2 \pmod{4}$.

Certainly if $k \equiv 2 \pmod{4}$ or $\ell \equiv 2 \pmod{4}$ we are done, so assume that both k and ℓ are divisible by 4. Since $k\ell - \deg \alpha = 1$, we see that $\deg \alpha$ is odd. Consider the automorphism

$$P = \begin{bmatrix} 1 & 0 \\ \alpha & 1 \end{bmatrix}$$

of A . Pulling back λ via P replaces L with

$$\begin{aligned} (P^*)^{-1}LP^{-1} &= \begin{bmatrix} 1 & -\overline{\alpha} \\ 0 & 1 \end{bmatrix} \begin{bmatrix} k & \overline{\alpha} \\ \alpha & \ell \end{bmatrix} \begin{bmatrix} 1 & 0 \\ -\alpha & 1 \end{bmatrix} \\ &= \begin{bmatrix} k + (\ell - 2)\overline{\alpha}\alpha & (1 - \ell)\overline{\alpha} \\ (1 - \ell)\alpha & \ell \end{bmatrix}. \end{aligned}$$

Since $\overline{\alpha}\alpha = \deg \alpha$ is odd and k and ℓ are divisible by 4, the upper left entry in this new array is congruent to 2 modulo 4. Thus, if a polarization is bad, it is isomorphic to a bad polarization λ for which either k or ℓ is congruent to 2 modulo 4.

Suppose λ is a bad polarization with $k \equiv 2 \pmod{4}$. Consider the polarization μ we obtain by taking Φ in diagram (2) to have kernel equal to the first group in (3); that is, we take Φ to be $\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}$. We compute that μ is given by the endomorphism

$$M = \begin{bmatrix} k/2 & \overline{\alpha} \\ \alpha & 2\ell \end{bmatrix},$$

whose upper left entry is odd, so μ is either good or split. Likewise, if $\ell \equiv 2 \pmod{4}$, we can take Φ in diagram (2) to have kernel equal to the second group in (3); that is, we take Φ to be $\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$. Then μ is given by the endomorphism

$$M = \begin{bmatrix} 2k & \overline{\alpha} \\ \alpha & \ell/2 \end{bmatrix},$$

whose lower right entry is odd, so μ is either good or split. This shows that in the graph G , every bad vertex is connected to at least one vertex that is good or split. To complete our argument, we need only show that bad vertices cannot be adjacent to split vertices.

If μ is a split polarization, then the polarized variety (A, μ) is isomorphic to a product surface $F_1 \times F_2$ with the product polarization, and both F_1 and F_2 have 2-rank equal to 1. If μ is connected to a good or a bad polarization, corresponding to a curve C , then C is obtained from F_1 and F_2 using the Howe–Leprévost–Poonen construction [19, Proposition 4]. Since F_1 and F_2 have rank 1, they have models of the form

$$F_1: \quad y^2 = (x^2 - n)(a_1x - b_1) \quad F_2: \quad y^2 = (x^2 - n)(a_2x - b_2),$$

where n is a nonsquare in \mathbf{F}_q . One computes that the curves obtained from F_1 and F_2 using the formulas of [19, Proposition 4] are of the form $y^2 = h$, where h is a sextic polynomial having 1 and -1 as roots. Thus, the vertices adjacent to a split vertex are either split or good. In particular, a bad vertex is never adjacent to a split vertex. \square

Justification of Heuristic Expectation 6.3. Take $d = 1$. We already noted that, under the GRH, the number of defect-1 elliptic curves over \mathbf{F}_q for 1-unexceptional q grows like $q^{1/4}$, up to logarithmic factors, and Heuristic Expectation 5.10 tells us to expect the number of genus-2 curves over \mathbf{F}_q of defect 2 produced by Algorithm 5.7 to grow like $q^{3/4}$, up to logarithmic factors. Proposition 6.4 tells us that at least $1/4$ of the curves produced by the algorithm can be written as $y^2 = f_1f_2$ for cubic polynomials f_1 and f_2 that are each compatible with at least $1/4$ of the defect-1 elliptic curves over \mathbf{F}_q .

For each genus-2 curve C in Step 9, we expect Algorithm 2.7 to succeed with probability on the order of $q^{-1/2}$, so we expect to have to apply Step 8 to about $q^{1/2}$ curves C before we succeed. Each application of Algorithm 2.7 takes time $\tilde{O}(q^{1/4})$, so the total time to success should be $\tilde{O}(q^{3/4})$. \square

7. RESULTS

We implemented our algorithms in Magma, and we ran Algorithm 6.1 on all of the odd prime powers less than 100,000. (This took a few days, running in the background on a modest laptop computer.) There are 9684 such prime powers q , four of which — 3^3 , 3^5 , 3^9 , and 5^5 — are 1-exceptional in the sense defined in Section 5. The genus-4 curves produced by the algorithm had

- defect 0 for 3027 of these q ($\approx 31.3\%$),
- defect 2 for 2268 of these q ($\approx 23.4\%$),
- defect 4 for 4054 of these q ($\approx 41.9\%$),
- defect 6 for 330 of these q ($\approx 3.4\%$), and
- defect 8 for 5 of these q ($\approx 0.05\%$).

The five q for which the best curve we found had defect 8 are the primes

$$154^2 + 3, \quad 160^2 + 160 + 3, \quad 221^2 + 16, \quad 282^2 + 282 + 5, \quad \text{and} \quad 307^2 + 4.$$

We maintain our conviction that for large enough 1-unexceptional q , our algorithm will find a curve of defect 4 or less — but q may have to be large indeed, because even though we expect the number of genus-2 defect-2 curves to grow like $q^{3/4}$, the implied constant is fairly small.

REFERENCES

- [1] Montserrat Alsina and Pilar Bayer, *Quaternion orders, quadratic forms, and Shimura curves*, CRM Monograph Series, vol. 22, American Mathematical Society, Providence, RI, 2004.
- [2] Z. I. Borevič and D. K. Faddeev, *Representations of orders with cyclic index*, Trudy Mat. Inst. Steklov **80** (1965), 51–65; English transl. in *Proceedings of the Steklov Institute of Mathematics. No. 80 (1965): Algebraic number theory and representations* (1968).
- [3] A. I. Borevich and I. R. Shafarevich, *Number theory*, Pure and Applied Mathematics, Vol. 20, Academic Press, New York–London, 1966. Translated from the Russian by Newcomb Greenleaf.
- [4] Reinier Bröker, *Constructing supersingular elliptic curves*, J. Comb. Number Theory **1** (2009), no. 3, 269–273.
- [5] Reinier Bröker, Everett W. Howe, Kristin E. Lauter, and Peter Stevenhagen, *Genus-2 curves and Jacobians with a given number of points*, LMS J. Comput. Math. **18** (2015), no. 1, 170–197, DOI [10.1112/S1461157014000461](https://doi.org/10.1112/S1461157014000461).
- [6] Nils Bruin and Kevin Doerksen, *The arithmetic of genus two curves with $(4, 4)$ -split Jacobians*, Canad. J. Math. **63** (2011), no. 5, 992–1024, DOI [10.4153/CJM-2011-039-3](https://doi.org/10.4153/CJM-2011-039-3).
- [7] Pierre Deligne, *Variétés abéliennes ordinaires sur un corps fini*, Invent. Math. **8** (1969), 238–243, DOI [10.1007/BF01406076](https://doi.org/10.1007/BF01406076).
- [8] Max Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hansischen Univ. **14** (1941), 197–272.
- [9] Mireille Fouquet and François Morain, *Isogeny volcanoes and the SEA algorithm*, Algorithmic number theory (Sydney, 2002) (C. Fieker and D. R. Kohel, eds.), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 276–291, DOI [10.1007/3-540-45455-1_23](https://doi.org/10.1007/3-540-45455-1_23), (to appear in print).
- [10] Gerard van der Geer and Marcel van der Vlugt, *Tables of curves with many points*, Math. Comp. **69** (2000), no. 230, 797–810, DOI [10.1090/S0025-5718-99-01143-6](https://doi.org/10.1090/S0025-5718-99-01143-6).
- [11] Josep González, Jordi Guàrdia, and Victor Rotger, *Abelian surfaces of GL_2 -type as Jacobians of curves*, Acta Arith. **116** (2005), no. 3, 263–287, DOI [10.4064/aa116-3-3](https://doi.org/10.4064/aa116-3-3).
- [12] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 4th ed., The Clarendon Press, Oxford University Press, New York, 1968. <http://archive.org/details/AnIntroductionToTheTheoryOfNumbers-4thEd-G.h.HardyE.m.Wright>.
- [13] Tsuyoshi Hayashida, *A class number associated with the product of an elliptic curve with itself*, J. Math. Soc. Japan **20** (1968), 26–43, DOI [10.2969/jmsj/02010026](https://doi.org/10.2969/jmsj/02010026).
- [14] Tsuyoshi Hayashida and Mieno Nishi, *Existence of curves of genus two on a product of two elliptic curves*, J. Math. Soc. Japan **17** (1965), 1–16, DOI [10.2969/jmsj/01710001](https://doi.org/10.2969/jmsj/01710001).
- [15] Everett W. Howe, *Principally polarized ordinary abelian varieties over finite fields*, Trans. Amer. Math. Soc. **347** (1995), no. 7, 2361–2401, DOI [10.2307/2154828](https://doi.org/10.2307/2154828).
- [16] ———, *New bounds on the maximum number of points on genus-4 curves over small finite fields*, Arithmetic, geometry, cryptography and coding theory, Contemp. Math., vol. 574, Amer. Math. Soc., Providence, RI, 2012, DOI [10.1090/conm/574/11431](https://doi.org/10.1090/conm/574/11431), (to appear in print).

- [17] E. W. Howe and K. E. Lauter, *Improved upper bounds for the number of points on curves over finite fields*, Ann. Inst. Fourier (Grenoble) **53** (2003), no. 6, 1677–1737, DOI [10.5802/aif.1990](#). Corrigendum: Ann. Inst. Fourier (Grenoble) **57** (2007), no. 3, 1019–1021, DOI [10.5802/aif.2284](#).
- [18] Everett W. Howe and Kristin E. Lauter, *New methods for bounding the number of points on curves over finite fields*, Geometry and arithmetic, EMS Ser. Congr. Rep., Eur. Math. Soc., Zürich, 2012, pp. 173–212, DOI [10.4171/119-1/12](#), (to appear in print).
- [19] Everett W. Howe, Franck Leprévost, and Bjorn Poonen, *Large torsion subgroups of split Jacobians of curves of genus two or three*, Forum Math. **12** (2000), no. 3, 315–364, DOI [10.1515/form.2000.008](#).
- [20] Everett W. Howe, Enric Nart, and Christophe Ritzenthaler, *Jacobians in isogeny classes of abelian surfaces over finite fields*, Ann. Inst. Fourier (Grenoble) **59** (2009), no. 1, 239–289, DOI [10.5802/aif.2430](#).
- [21] M. Kaneko and D. Zagier, *Supersingular j -invariants, hypergeometric series, and Atkin’s orthogonal polynomials*, Computational perspectives on number theory (Chicago, IL, 1995), AMS/IP Stud. Adv. Math., vol. 7, Amer. Math. Soc., Providence, RI, 1998, pp. 97–126.
- [22] Ernst Kani, *Products of CM elliptic curves*, Collect. Math. **62** (2011), no. 3, 297–339, DOI [10.1007/s13348-010-0029-1](#).
- [23] David Russell Kohel, *Endomorphism rings of elliptic curves over finite fields*, Ph.D. Thesis, University of California, Berkeley, 1996.
- [24] Gilles Lachaud, Christophe Ritzenthaler, and Alexey Zykin, *Jacobians among abelian three-folds: a formula of Klein and a question of Serre*, Math. Res. Lett. **17** (2010), no. 2, 323–333, DOI [10.4310/MRL.2010.v17.n2.a11](#).
- [25] J. E. Littlewood, *On the Class-Number of the Corpus $P(\sqrt{-k})$* , Proc. London Math. Soc. **S2-27**, no. 1, 358, DOI [10.1112/plms/s2-27.1.358](#).
- [26] Jean-François Mestre, *Courbes de genre 3 avec S_3 comme groupe d’automorphismes* (2010). [arXiv:1002.4751 \[math.AG\]](#).
- [27] Kenneth A. Ribet, *Bimodules and abelian surfaces*, Algebraic number theory (J. Coates, R. Greenberg, B. Mazur, and I. Satake, eds.), Adv. Stud. Pure Math., vol. 17, Academic Press, Boston, MA, 1989, pp. 359–407.
- [28] René Schoof, *Nonsingular plane cubic curves over finite fields*, J. Combin. Theory Ser. A **46** (1987), no. 2, 183–211, DOI [10.1016/0097-3165\(87\)90003-3](#).
- [29] Jean-Pierre Serre, *Sur le nombre des points rationnels d’une courbe algébrique sur un corps fini*, C. R. Acad. Sci. Paris Sér. I Math. **296** (1983), no. 9, 397–402. = Œuvres [128]. [http://gallica.bnf.fr/ark:/12148/bpt6k31623/f592](#).
- [30] ———, *Nombres de points des courbes algébriques sur \mathbf{F}_q* , Seminar on number theory, 1982–1983 (Talence, 1982/1983), Univ. Bordeaux I, Talence, 1983, pp. Exp. No. 22, 8. = Œuvres [129].
- [31] ———, *Résumé des cours de 1983–1984*, Ann. Collège France (1984), 79–83. = Œuvres [132].
- [32] Andrew V. Sutherland, *Computing Hilbert class polynomials with the Chinese remainder theorem*, Math. Comp. **80** (2011), no. 273, 501–538, DOI [10.1090/S0025-5718-2010-02373-7](#).
- [33] John Voight, *Quaternion algebras*. To appear in the Springer Graduate Texts in Mathematics series.
- [34] William C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4) **2** (1969), 521–560. [http://www.numdam.org/item?id=ASENS_1969_4_2_4_521_0](#).
- [35] André Weil, *Sur les fonctions algébriques à corps de constantes fini*, C. R. Acad. Sci. Paris **210** (1940), 592–594. [http://gallica.bnf.fr/ark:/12148/bpt6k31623/f592](#).
- [36] ———, *On the Riemann hypothesis in function-fields*, Proc. Nat. Acad. Sci. U. S. A. **27** (1941), 345–347. [http://www.pnas.org/content/27/7/345.short](#).
- [37] ———, *Sur les courbes algébriques et les variétés qui s’en déduisent*, Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg **7** (1945), Hermann et Cie., Paris, 1948.
- [38] ———, *Variétés abéliennes et courbes algébriques*, Actualités Sci. Ind., no. 1064 = Publ. Inst. Math. Univ. Strasbourg **8** (1946), Hermann & Cie., Paris, 1948.
- [39] P. J. Weinberger, *Exponents of the class groups of complex quadratic fields*, Acta Arith. **22** (1973), 117–124. [http://pldml.icm.edu.pl/pldml/element/bwmeta1.element.bwnjournal-article-aav22i2p117bwm](#).

CENTER FOR COMMUNICATIONS RESEARCH, 4320 WESTERRA COURT, SAN DIEGO, CA 92121,
USA

E-mail address: `however@alumni.caltech.edu`

URL: `http://www.alumni.caltech.edu/~however/`